

Meslek Yüksekokulu Öğrencilerinin Siber Güvenliğe Yönelik Farkındalıklarının Belirlenmesi: Ordu Üniversitesi Örneği

Servet KILIÇ¹ 

Öz

Bu çalışmada, Meslek Yüksekokulu öğrencilerinin siber güvenliğe yönelik farkındalık düzeylerinin belirlenmesi amaçlanmıştır. Bu çerçevede öğrencilerin; cinsiyetleri, bölümleri, internet kullanım sıklıkları ve amaçları dikkate alınmıştır. Çalışma nicel araştırmalar arasında yer alan tarama yöntemiyle yürütülmüştür. Çalışmaya teknik ve sosyal bilimlerde öğrenim gören 403 öğrenci katılmıştır. Elde edilen nicel veriler üzerinde yapılan normal dağılım testleri sonrası, bulgular parametrik olmayan testler (Mann Whitney U Testi, Kruskal Wallis Testi) yoluyla elde edilmiştir. İnternet kullanım sıklığı ile ilgili veriler betimsel istatistik tekniklerine göre analiz edilmiş, bulgular yüzde ve frekans değerleri ile sunulmuştur. Elde edilen bulgulara göre; teknik ve sosyal bilimlerde öğrenim gören öğrencilerin siber güvenlik farkındalıkları yüksek düzeydedir. Özellikle Bilgisayar Teknolojileri, Hakla İlişkiler ve İşletme Yöntemi bölümü öğrencileri diğerlerinden pozitif olarak farklılaşmıştır. Turizm bölümü öğrencilerinin siber güvenlik farkındalık düzeyi yüksek olmakla birlikte diğerlerine oranla daha düşüktür. Cinsiyet ve internet kullanım faktörü öğrencilerin farkındalık düzeylerini etkilememiştir. Öğrenciler interneti daha çok; bilgi edinme, sosyal medya, oyun ve eğlence amaçlı olarak kullanmaktadır.

Anahtar kelimeler: Siber güvenlik, meslek yüksekokulu, farkındalık.

Geliş: 15 Nisan 2025, **Kabul:** 18 Mayıs 2025, **Yayın:** 25 Haziran 2025

Determining the Awareness of Vocational School Students Regarding Cybersecurity: The Example of Ordu University

Abstract

This study aims to determine the cybersecurity awareness levels of vocational school students. In this context, the students' gender, departments, Internet usage frequency and purposes were taken into consideration. The study was conducted using the scanning method, which is among the quantitative studies. 403 students studying technical and social sciences participated in the study. After the normal distribution tests were performed on the quantitative data, the findings were obtained through nonparametric tests (Mann-Whitney U test, Kruskal Wallis test). Data on Internet usage frequency were analyzed using descriptive statistics techniques, and the findings were presented with percentage and frequency values. According to the findings the cybersecurity awareness levels of students studying technical and social sciences were high. Especially the students of computer technologies, public relations and business method departments differed positively from the others. Although the cybersecurity awareness level of tourism department students was high, it was lower than that of the others. Gender and Internet usage did not affect students' awareness levels. Students mostly used the Internet for information, social media, games and entertainment purposes.

Keywords: Cyber security, vocational school, awareness.

Received: 15 April 2025, **Accepted:** 18 May 2025, **Published:** 25 June 2025

¹ Ordu Üniversitesi, Teknik Bilimler Meslek Yüksekokulu, Ordu, servetkili@odu.edu.tr

Atıf: Kılıç, S. (2025). Meslek yüksekokulu öğrencilerinin siber güvenliğe yönelik farkındalıklarının belirlenmesi: Ordu Üniversitesi örneği. *İhlara Eğitim Araştırmaları Dergisi* 10(1), 101-112. <https://doi.org/10.47479/ihead.1676690>



© İhlara Eğitim Araştırmaları Dergisi. This is an open-access article under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (<https://creativecommons.org/licenses/by-nc-sa/4.0/>).

Giriş

Teknolojinin hızlı gelişmesiyle birlikte dijital araçlar ve ortamlar hayatın birçok alanında kullanılmaya başlanmıştır. Bilgi iletişim teknolojilerinde yaşanan değişimler bilgisayar ve internet kullanımını da artırmıştır. Bireyler kişisel verileri, maddi varlıkları ve sağlık gibi bilgilerini dijital ortamda tutarken, günlük yaşantılarını ve düşüncelerini de kendi istekleriyle bu ortamlarda paylaşmaktadır. Özellikle sosyal ağların (Facebook, Instagram, X, TikTok) kolay erişilebilir olması, birçok kitlenin bu ağları bilgi paylaşımı ve iletişim kanalı haline gelmiştir (Arıcak vd., 2012, Aslan, 2020). Bu durumun birçok avantajı olmasının yanı sıra, bilgilerin güvenliğine yönelik endişeleri de beraberinde getirmektedir. İnternet kullanımının artmasıyla birlikte siber tehdit ve saldırılara maruz kalan kullanıcı sayısı da artmakta olup, siber suçlar teknolojik gelişmelerle birlikte çeşitlenmekte ve artmaktadır (Salem vd., 2021). Kişilerin bilgisi ve izni dışında veriler diğer şahıslar tarafından paylaşılabilir ve farklı amaçlarla kullanılabilir. Banka hesaplarına erişim yapılarak hesap bakiyesi sıfırlanabilir. Sosyal medya şifreleri ele geçirilerek kişinin bilgisi dışında yüz kızartıcı paylaşımlar yapılabilir. Bu gibi beklenmedik ve istenmeyen güvenlik zafiyetleri sonrasında, kişiler toplum önünde olumsuz durumlara düşürülebilir, hukuki olarak yaptırımlara veya cezalara maruz kalabilir. Özellikle çocuklar ve gençler saldırıya, şiddete ve çeşitli zorbalıklara maruz kalabilir (Eroğlu, 2014).

Sanal ortamlarda olumsuzlukların önlenmesinde siber güvenlik günümüzde büyük bir önem taşımaktadır. Siber güvenlik, yapılan her türlü saldırıların belirlenmesi, önlenmesi ve çeşitli önlemler alınarak bilgilerin korunmasıdır (Barrett, 2018). Daha kapsamlı bir yaklaşımla siber güvenlik; kişilerin her türlü haklarını ve varlıklarını korumak amacıyla benimsenebilecek politikaları, kullanılabilir araçları, güvenlik önlemlerini, risk yönetimlerini, eylemleri ve uygulamaları içermektedir (International Telecommunication Union, 2008). Siber güvenliğin sağlanmadığı ortamlarda yapılan saldırılar, veri ihlalleri ve kimlik hırsızlıkları; kişisel bilgilerin ve kurumsal verilerin güvenliğini tehdit etmektedir. Bu nedenle siber güvenlik, sadece teknoloji dünyasında çalışan profesyonellerin değil, tüm bireylerin ve kuruluşların öncelikli sorumluluğu haline gelmiştir.

Siber güvenlik zafiyetleri sonrası kişiler; siber zorbalık, taciz ve istismar gibi olumsuzluklara da maruz kalabilirler. Siber zorbalık, sanal ortamlarda bilgi ve iletişim teknolojileri yoluyla özel veya tüzel kişilere karşı yapılan teknik, psikolojik ve fiziksel olarak verilen zararlar (Arıcak, 2011; Barlet ve Chamberlin, 2017). Sosyal medyada asılsız ve alay edici paylaşımlar yapılarak dalga geçilmesi ve iftiralar atılması (Süslü, 2016), oyun veya doğrudan iletişim amacıyla kullanılan mesajlaşma platformlarında; incitici, hakaret, taciz ve tehdit içerikli mesajlar yazmak (Süslü, 2016), fidye yazılımları yoluyla bilgilerin ele geçirilmesi ve kişilerden fidye talep edilmesi (Hatipoğlu ve Tunacan, 2021) gibi durumlar siber zorbalığa örnek gösterilebilir. Sosyal medya platformlarında çok fazla vakit geçiren ve internet kullanım süresi artan bireylerin zorbalığa maruz kalma ihtimalleri de artabilmektedir (Türk ve Şenyuva, 2021). Akıllı telefonların yaygınlaşmasıyla birlikte internet ortamında sıkça vakit geçiren farklı yaş gruplarındaki bireyler doğrudan ve dolaylı olarak zorbalıklara maruz kalabilirler (Chen vd., 2017). Öte yandan bazı araştırmacılar, internette daha fazla vakit geçiren kişilerin, teknolojiye dair becerilerini daha fazla geliştirebileceklerini ifade etmektedir (Özbek, 2019). Bu, onları potansiyel tehditlere karşı daha dikkatli ve bilinçli hale getirebilir. Örneğin, bir öğrenci sürekli olarak dijital araçlarla ilgilenirken; antivirüs yazılımları, VPN kullanımı veya şüpheli e-postalarla ilgili daha fazla bilgi edinebilir. Bu tür öğrencilerin siber güvenlik farkındalıkları da zamanla artabilir. Özellikle sosyal medya, video izleme ve oyun oynama gibi platformlarında geçirilen zaman, öğrencilerin çevrimiçi ortamlarda karşılaştıkları tehlikeler hakkında farkındalık yaratabilir.

Siber zorbalık olarak başlayan ve daha sonra siber tacize dönüşen durumlara da rastlanmaktadır. Siber tacizin görülme sıklığı cinsiyete bağlı olarak da değişiklik gösterebilir. Toplumda kadınların ve erkeklerin teknolojiye olan ilgisi ve bu alandaki becerileri farklı olabilir. Bu durum, kadınların siber güvenlik tehditlerini daha fazla önemsemelerine neden olabilir. Kadınlar, çevrimiçi ortamda daha fazla cinsiyet temelli saldırılarla karşılaşabilirler. Cinsiyet temelli saldırılar, kadınların siber güvenliğe olan yaklaşımını etkileyebilir ve onları dijital dünyada daha temkinli hale getirebilir. Çevrimiçi ortamlarda özellikle kız çocuklarına ve kadınlara siber taciz şeklinde başlayarak cinsel tacize kadar giden vakalara rastlanmaktadır (Doğan vd., 2018). Yaman ve Sönmez (2015) ergenlerin siber zorbalık eğilimlerini belirlemeyi amaçladığı çalışmada, ergenlerin siber zorbalık eğilimlerinin cinsiyete göre değiştiğini belirtmişlerdir. Özer Öksüzöğlu (2021) kadınlara yönelik siber zorbalık durumlarını ve önleme çabalarını ele aldığı çalışmada, en fazla dikkat çeken konulardan birisinin kadınlara yönelik cinsel saldırılar olduğunu ifade etmiştir.

Literatürde farklı yaş gruplarındaki öğrenciler için yapılan siber güvenlik çalışmalarına rastlanmaktadır. Şener vd. (2022) pandemi sürecinde siber güvenlik farkındalıkları kapsamında üniversite öğrencilerinin siber zorbalık ve siber mağduriyet düzeylerini belirlemeye çalışmışlardır. Edinilen sonuçlarda, öğrencilerin yaklaşık yüzde 30'unun siber mağduriyet yaşadıkları görülmüştür. Özbek (2019) hizmet öncesi öğretmenlerinin kişisel siber güvenlik sağlama durumlarını incelemiştir. Araştırma sonuçlarına göre; öğretmen adaylarının siber güvenlik farkındalıklarının orta düzeyde olduğu bulunmuştur. Ayrıca erkek adayların siber güvenlik farkındalıklarının, kadın adaylardan yüksek olduğu ifade edilmiştir. Yine interneti daha sık kullanan adayların farkındalıklarının daha yüksek olduğu belirtilmiştir. Moallem (2019), üniversite öğrencilerinin siber güvenlik farkındalıklarını araştırdığı çalışmada, öğrencilerin kişisel verilerini nasıl koruyacakları konusunda çok fazla bilgi sahibi olmadıklarını vurgulamıştır. Bhatnagar ve Pry (2020), öğrencilerin sosyal medya sitelerinin kişisel gizliliği ve siber güvenliğine ilişkin tutumlarını, farkındalıklarını ve algılarını belirlemiştir. Bulgular, öğrencilerin sosyal medya platformlarının kullanımındaki gizlilik ve güvenlik risklerinin farkında olduklarını, bu alanda ek eğitime değer verdiklerini ve bunu önerdiklerini göstermiştir.

Siber güvenlik farkındalığı oluşmamış ve tehditleri önlemeye yönelik bilgisi sınırlı olan kişilerin olumsuz durumlarla karşılaşma olasılığının daha yüksek olduğu söylenebilir. Siber saldırıların artan sıklığı, güvenlik yazılımlarının yeterli olmadığını ve internet kullanıcılarının siber güvenlik bilgisiyle donatılması gerektiğini ortaya koymaktadır (Aksoğan vd. 2018). Siber güvenlik ile ilgili farkındalığın oluşmasında teknik bilgilerin yanı sıra psikolojik etmenler de etkili olabilir. Bireylerin siber tehditleri algılaması, kişilik özellikleri, risklere karşı tepkileri ve güvenlik önlemlerini uygulama motivasyonları psikolojik faktörlerle doğrudan ilişkilidir (Yiğit ve Seferoğlu, 2019). Üniversite öğrencileri üzerinde yapılan bir çalışma, A/B tipi kişilik özelliklerinin siber güvenlik farkındalığı üzerinde etkili olduğunu göstermiştir (Şimşek, 2024). Bireylerin siber tehditleri algılamaları ve bu tehditlere karşı verdikleri tepkiler, güvenlik davranışlarını etkileyebilir. Örneğin, kimlik avı saldırılarını hafife alan bireyler, gerekli önlemleri almayabilirler (Bada vd., 2019). Dolayısıyla bireylerin daha bilinçli olması ve her türlü olumsuzluklara karşı gerekli tedbirleri alması gereklidir.

Günümüzde ilkokuldan üniversiteye kadar farklı eğitim kademelerinde öğrenim gören öğrencilere siber güvenlik ve güvenli internet kullanımı noktasında bilgilendirme çalışmaları yapılmaktadır. Özellikle üniversitelerde öğrenim gören öğrencilerin siber güvenliğe ilişkin farkındalıklarını ortaya koymak ve onları bilgilendirici ve eğitici çalışmalar yapmak oldukça önemlidir (Özbek, 2019; Şener vd., 2022). Üniversitelerde farklı alanlarda ve bölümlerde öğrenim gören öğrencilerin siber güvenlik farkındalıkları değişkenlik gösterebilir. Bilgisayar, tablet veya telefon gibi araçlarla interneti sadece ihtiyaç için kullanan öğrencilerin yanı sıra, belirli bir amaç için kullanan öğrencilerin siber güvenlik uygulamaları değişebilir. Özellikle meslek yüksekokullarında hem teknik bilimlere hem de sosyal bilimlere ait bölümlerin olması, öğrencilerin siber güvenlik farkındalıklarının alan farklılıklarına göre nasıl değiştiği noktasında önemli bilgiler verebilir. Bilgisayar teknolojisi ile ilgili bölümler bilgisayar ağları, yazılım geliştirme, sistem güvenliği ve şifreleme gibi konuları ele alır. Bu öğrenciler genellikle siber güvenliği teknik bir konu olarak ele alır ve siber saldırılar, güvenlik protokolleri ve ağ güvenliği gibi konularda daha fazla bilgi sahibidirler. Elektrik ve elektronik ile ilgili bölümler genellikle donanım ve sistemlerle ilgilenirler. Bu bölümlerde eğitim gören öğrenciler, siber güvenliği daha çok donanım güvenliği ve fiziksel cihazlar üzerinden düşünürler. Siber güvenlik algıları; donanımın güvenliği, sistemin korunması ve sensörler gibi teknolojilerle ilişkilidir. Otomotiv teknolojileri, mobilya, tekstil, işletme, iktisat ve halkla ilişkiler gibi alanlarda siber güvenlik eğitimi daha az yer tutabilir. Ancak dijitalleşmenin arttığı ve teknolojinin her sektörde daha fazla yer aldığı düşünüldüğünde, bu bölümlerde de temel siber güvenlik farkındalıklarının ortaya konulması gerekli görülebilir.

Öğrencilerin öğrenim gördükleri bölüme bağlı olarak siber güvenlik farkındalıklarındaki değişimi anlamak, eğitim programlarının ne derece etkili olduğunu ve hangi alanlarda iyileştirme yapılması gerektiğini değerlendirmek için önemlidir. Bu nedenle güvenlik sorunlarını azaltmak veya önlemek için öğrencilerin farkındalığı artırmak ve insanları güvenlik konusunda eğitmek gereklidir (Kovačević vd., 2020). Öğrencilerin siber güvenlik uygulamalarının doğru bir şekilde belirlenmesi, siber saldırılara karşı daha hazırlıklı olmalarına ve güvenli bir dijital yaşam sürmelerine yardımcı olabilir. Elde edilen bulgular, okul yöneticilerine ve eğitimcilere siber güvenliğin önemi ve eğitimi noktasında bir farkındalık oluşturabilir. Kullanıcıların siber güvenlik ve güvenli kullanım becerisi bilgisi eksikliği, siber ortamda kendilerini güvensiz hissetmelerine neden olmaktadır. Bu kapsamda bu çalışmada, Meslek Yüksekokulu öğrencilerinin siber güvenliğe yönelik farkındalık düzeylerinin belirlenmesi amaçlanmıştır.

Araştırma Soruları

1. Meslek Yüksekokulu öğrencilerinin cinsiyete bağlı olarak siber güvenlik farkındalık düzeyleri nasıl değişmektedir?
2. Meslek Yüksekokulu öğrencilerinin bölümlerine bağlı olarak siber güvenlik farkındalık düzeyleri nasıl değişmektedir?
3. Meslek Yüksekokulu öğrencilerinin internet kullanım sıklıklarına bağlı olarak siber güvenlik farkındalık düzeyleri nasıl değişmektedir?
4. Meslek Yüksekokulu öğrencilerinin interneti kullanım amaçları nasıl çeşitlenmektedir?

Yöntem

Araştırma nicel araştırmalar arasında yer alan tarama yöntemiyle yürütülmüştür. Tarama araştırmaları diğer araştırmalara göre daha büyük örneklem grubunun görüşlerini ya da özelliklerini (Bilgi, ilgi, algı, farkındalık, kaygı, tutum, inanç vb.) betimlemek amacıyla yapılmaktadır (Fraenkel ve Wallen, 2006). Veriler, belirli bir zamana yayılmadan anlık olarak topluluğun her bireyinden değil bir kitleyi temsil eden parçasından kesitsel olarak toplanmıştır (Fraenkel ve Wallen, 2006.).

Katılımcılar

Katılımcıların belirlenmesinde; yüz yüze kolay ulaşılabilir olması, gönüllülüğe bağlı olması ve yeterli örnekleme sahip olunması gibi nedenlerden dolayı amaçlı örnekleme yöntemleri arasında yer alan uygun örnekleme tekniği tercih edilmiştir (Teddle ve Yu, 2007). Bu çerçevede araştırmanın örneklemini Ordu ili merkez ve ilçelerinde Üniversitenin teknik ve sosyal bilimlerinde öğrenim gören meslek yüksekokulu öğrencileri oluşturmaktadır. Öğrenciler cinsiyet, bölüm ve internet kullanım sıklığı durumlarına göre kategorize edilmiştir. Tablo 1'de öğrencilerin demografik bilgileri yer almaktadır.

Tablo 1. Öğrencilerin demografik özellikleri.

Kategori	Demografik Bilgi	N
Cinsiyet	Erkek	244
	Kadın	159
Bölüm	Bilgisayar Teknolojileri	115
	Elektronik Teknolojisi	46
	Halk ve İlişkiler	31
	İnşaat Teknolojileri	48
	İşletme Yönetimi	35
	Makine ve Metal Teknikleri	34
	Mimari Dekoratif	32
	Muhasebe	32
	Turizm	30
İnternet Kullanım Sıklığı	3 saat altı	79
	3-5 saat	217
	5 saat üstü	107
Toplam		403

Tablo 1’deki veriler incelendiğinde örneklem içerisinde erkekler (N=244), Bilgisayar Teknoloji bölümü (N=115) ve 3-5 saat arası internet kullanan öğrenciler (N=217) çoğunluktadır. İnternet kullanım sıklığı ile ilgili belirlenen seçenekler daha önce yapılan çalışmalar referans alınarak belirlenmiştir (Şener vd., 2022).

Veri Toplama Araçları

Veri toplama aracı olarak Arpacı ve Sevinc (2022) tarafından geliştirilen siber güvenlik ölçeği kullanılmıştır. Ölçeğin Türkçe versiyonu yazardan e posta yoluyla istenmiş ve ölçek kullanım izni alınmıştır. 25 maddeden oluşan ölçek 5’li likert tipinde hazırlanmıştır. Maddeler “kesinlikle katılmıyorum (1 puan)” ve “kesinlikle katılıyorum (5 puan)” arasında seçeneklere ayrılmış ve puanlandırılmıştır. Toplam sekiz ters madde bulunan ölçekte puanlamalar da ters yapılmıştır. Ölçekten alınabilecek en düşük puan 25 iken, en yüksek puan 125’tir. Ölçeğin Cronbach alfa iç tutarlık katsayısı 0.88’dir. Ölçek verileri toplanırken öğrencilerin internet kullanım amacını ortaya koymak amacıyla demografik bilgi de alınmıştır. Seçenekler arasında; eğitim ve araştırma, sosyal medya, eğlence ve diğer şeklinde maddeler yer almıştır. Diğer seçenek açık uçlu olarak verilmiştir.

Verilerin Analizi

Öğrencilerin genel farkındalık düzeyini belirleyebilmek için değerlendirme ölçütü ortaya konmuştur (Tablo 2).

Tablo 2. MYO öğrencilerinin siber güvenlik farkındalık düzeylerini değerlendirme ölçütü.

Ölçek birimi aralığı	Ölçek toplam puanı aralığı	Değerlendirme Ölçüt Düzeyi
1.00 - 1.79	25 - 45	Çok düşük
1.80 - 2.59	46 - 65	Düşük
2.60 - 3.39	66 - 85	Orta
3.40 - 4.19	86 - 105	Yüksek
4.20 - 5.00	106 - 125	Çok Yüksek

Tablo 2’de belirtilen ölçütler Özbek (2019) tarafından yürütülen çalışmadan referans alınmıştır. Ölçeğin her bir maddesine verilen puan aralıkları ve tüm maddelerden elde edilen toplam puan birlikte değerlendirilerek bir ölçüt ortaya konmuştur.

Bağımsız değişkenlere bağlı olarak ölçekten elde edilen verilerin normal dağılım gösterip göstermediğini belirlemek amacıyla öncelikle normallik testi yapılmıştır. Kolmogorov-Smirnov (0.061, $p < 0.05$) ve Shapiro Wilk (0.939, $p < 0.05$) test sonuçları sonrasında siber güvenlik ölçeğinden elde edilen puanlar normal dağılım göstermemiştir. Cinsiyet değişkenine bağlı puanlar incelendiğinde, kadınlardan elde edilen puanlar normal dağılım göstermemiştir (0.099, $p < 0.05$). İnternet kullanım sıklığı değişkenine bağlı puanlar incelendiğinde, 1-3 saat (0.086, $p < 0.05$) ve 3-5 saat (0.073, $p < 0.05$) puanları normal dağılım göstermemiştir. Bölüm değişkenine bağlı olarak puanlar incelendiğinde, Bilgisayar (0.089, $p < 0.05$), İşletme Yönetimi (0.157, $p < 0.05$), Makine ve Metal Teknolojileri (0.158, $p < 0.05$) ve Mimari Dekoratif (0.145, $p < 0.05$) puanları normal dağılım göstermemiştir. Normallik test sonuçlarına bağlı olarak puanlar üzerinde parametrik olmayan testler uygulanmıştır. Cinsiyet puanları arasındaki farkı incelemek için Mann Whitney U testi, internet kullanım sıklığı ve bölüm puanları arasındaki farkları incelemek için Kruskal Wallis testi yapılmıştır. Mann Whitney U testi bağımsız iki bağımsız değişkenin ortanca değerlerini karşılaştırmak için kullanılır (Kalaycı, 2016). Kruskal Wallis testi üç veya daha fazla bağımsız değişkenin ortanca değerlerini karşılaştırmak için kullanılır (Kalaycı, 2016). Öğrencilerin internet kullanım amacını belirlemek amacıyla betimsel analiz yapılmış ve verilerin frekans ile yüzdeleri hesaplanmıştır.

Bulgular

Araştırma soruları çerçevesinde bulgular kategorize edilmiştir. Öncelikle bağımsız değişkenler ile ilgili ortalamalara bağlı olarak ortaya çıkan tüm tanımlayıcı istatistiksel bulgular çıkarılmıştır. Daha sonra veriler üzerinde parametrik olmayan testler yapılarak ortancaya bağlı olarak anlamlı farklılıkların olup olmadığına dair bulgular tablolar halinde sunulmuştur. Tablo 3'teki bulgulara göre; cinsiyete, bölüme ve internet kullanım sıklığına bağlı olarak MYO öğrencilerinin siber güvenlik farkındalık düzeyleri yüksektir (Yüksek düzey puan aralığı: 86-105).

Tablo 3. Bağımsız değişkenlere bağlı tanımlayıcı istatistik analiz bulguları.

Kategori	Değişkenler	N	M	Sd
Cinsiyet	Erkek	244	98.21	11.45
	Kadın	159	97.16	12.46
Bölüm	Bilgisayar Teknolojileri	115	101.39	8.22
	Elektronik Teknolojisi	46	97.8	10.8
	Halk ve İlişkiler	31	99.45	11.89
	İnşaat Teknolojileri	48	93.72	13.32
	İşletme Yönetimi	35	100.54	15.53
	Makine ve Metal Teknikleri	34	93.29	14.7
	Mimari Dekoratif	32	95.06	15.27
	Muhasebe	32	96.96	9.77
	Turizm	30	94.6	7.37
	İnternet Kullanım Sıklığı	3 saat altı	79	99.68
	3-5 saat	217	96.52	11.71
	5 saat üstü	107	99.01	10.24

Cinsiyete Bağlı Olarak Öğrencilerin Siber Güvenlik Farkındalıklarına Yönelik Bulguları

Erkek ve kadın öğrencilerin siber güvenlik ortanca puanları ve puan farklılıklarının anlamlı olup olmadığını gösteren bulgular Tablo 4'te verilmiştir. Mann Whitney U testi sonuçlarına göre erkek öğrencilerin test puanları (Ortc.=98.5), kadınların test puanlarından (Ortc.=97) yüksektir. Elde edilen bu bulgulara göre değişkenler arasında anlamlı bir farklılık ortaya çıkmamıştır (U=18081.5, p>0.05).

Tablo 4. Cinsiyete bağlı bulgular.

Cinsiyet	N	Ortc.	Sıralar Ortalaması	U	p
Erkek	244	98.5	207.4	18081.5	.249
Kadın	159	97	193.72		

İnternet Kullanım Sıklığına Bağlı Olarak Öğrencilerin Siber Güvenlik Farkındalıklarına Yönelik Bulguları

Farklı sıklıkta internet kullanan MYO öğrencilerinin siber güvenlik ortanca puanları ve puan farklılıklarının anlamlı olup olmadığını gösteren bulgular Tablo 5'te sunulmuştur. Kruskal Wallis testi sonuçlarına göre öğrencilerin internet kullanım sıklığı; 1 ile 3 saat arası (Ortc.=99), 5'ten fazla saat (Ortc.=98) ve 3 ile 5 saat arası (Ortc.=97) olarak sıralanmaktadır. Puanlar arasındaki bu farklılıklara rağmen bu sonuçlar anlamlı bir fark ortaya koymamıştır (H(2)=4.455, p>0.05).

Tablo 5. İnternet kullanım sıklığına bağlı bulgular.

İnternet Kullanım Sıklığı	N	Ortc.	H	p
1-3 saat	79	99	4.455	.108
3-5 saat	217	97		
5+ saat	107	98		

Bölgümlere Bağlı Olarak Öğrencilerin Siber Güvenlik Farkındalıklarına Yönelik Bulguları

Farklı bölümlerde öğrenim gören MYO öğrencilerinin siber güvenlik ortanca puanları ve puan farklılıklarının anlamlı olup olmadığını gösteren bulgular Tablo 6'da gösterilmiştir. Kruskal Wallis testi sonuçlarına göre bölümlere bağlı olarak öğrencilerin siber güvenlik farkındalıkları arasında anlamlı bir fark vardır (H(8)= 26.921, p<0.05). Anlamlı farklılıkların hangi bölümler arasında olduğunu gösteren Tablo 7'ye göre Bilgisayar bölümü öğrencilerinin siber güvenlik farkındalıkları genel olarak diğer bölümlere göre daha yüksektir. Turizm bölümü öğrencilerinin ise siber güvenlik farkındalıkları genel olarak daha düşüktür.

Tablo 6. Bölümlere bağlı bulgular.

Bölüm	N	Ortc.	H	p
Bilgisayar Teknolojileri	115	101	26.921	.001
Elektronik Teknolojisi	46	97.5		
Halk ve İlişkiler	31	99		
İnşaat Teknolojileri	48	95		
İşletme Yönetimi	35	98		
Makine ve Metal Teknikleri	34	94		
Mimari Dekoratif	32	96.5		
Muhasebe	32	98		
Turizm	30	93.5		

Tablo 7. Bölümler arasında oluşan puan farklılıkları için çiftler arası karşılaştırma bulguları.

Bölüm	Bilgisayar Teknolojileri (p)	İşletme Yönetimi (p)	Halk ve İlişkiler (p)
İnşaat Teknolojileri	.000**		.047*
Makine ve Metal Teknikleri	.001*		
Mimari Dekoratif	.027*		
Muhasebe	.025*		
Turizm	.000**	.028*	.025*

* p<0.05, ** p<0.01

Öğrencilerin İnterneti Kullanım Amaçlarına Yönelik Bulguları

Ölçek doldurma sürecinde 403 öğrenciden internet kullanım amaçlarının belirlenmesi istenmiştir. Ortaya konulan bu bulgulara öğrenciler birden fazla seçeneği işaretleyebilmişlerdir. Tablo 8'e göre, öğrencilerin yüzde 38'i (N=152) bilgi edinmek, neredeyse yarısı sosyal medya (N=196, % 48) ve yüzde 31'i (N=126) oyun ve eğlence için interneti kullanmaktadır.

Tablo 8. Öğrencilerin internet kullanım amaçları.

	Frekans (f)	Yüzde (%)
Bilgi edinme	46	11
Bilgi edinme- Sosyal medya	83	21
Bilgi edinme- Oyun ve eğlence	23	6
Sosyal medya	113	28
Sosyal medya-Oyun ve eğlence	43	10
Oyun ve eğlence	60	15
Vakit geçirme	35	9
Toplam	403	100

Tartışma

Bu çalışmada Meslek Yüksekokulu öğrencilerinin siber güvenlikle ilgili farkındalık düzeyleri ortaya konulmuştur. Genel olarak öğrencilerin siber güvenlik farkındalıklarının yüksek olduğu görülmüştür. Öğrencilerin yüzde 38'i interneti bilgi edinmek amaçlı olarak kullanmaktadır. Bilgi sağlayan güvenilir birçok site olmasına karşın kötü amaçlı olarak bilgi sağlayan birçok internet sitesi de mevcuttur. Bu süreçte çoğu öğrenci iyi veya kötü deneyimler yaşayabilmektedir. Yaşanan deneyimler öğrencilerin siber güvenlik bilinç ve farkındalık düzeylerini artırmada etkili olabilir (Özbek, 2019).

Ayrıca bu çalışmada öğrencilerin neredeyse yarısı sosyal medya kullandıklarını belirtmiştir. Sosyal medyadan öğrencileri bilinçlendirmeye yönelik farklı türden yararlı bilgiler edinilebildiği gibi bu platformlarda bilgi gizliliği ve güvenliğini etkileyebilecek unsurların da yer aldığı bilinmektedir. Literatürde üniversite öğrencilerinin sosyal medyadan gizlilik ve güvenliğe ilişkin gelebilecek tehditlerin farkında oldukları belirtilmiştir (Bhatnagar ve Pry, 2020).

Cinsiyete bağlı olarak MYO öğrencilerinin siber güvenlik farkındalıkları arasında bir fark olmadığı, fakat her ikisinin de farkındalık düzeylerinin yüksek olduğu görülmüştür. Literatürde siber güvenlik ve tehditlerine yönelik yürütülen çalışmalarda farklı sonuçlar elde edilmiştir. Bazı çalışmalarda cinsiyetin etkili olmadığı belirtilirken (Karacı vd., 2017; Korkmaz, 2016), bazı çalışmalarda etkili olduğu vurgulanmaktadır (Özbek, 2019). Kadınlar çevrimiçi ortamlarda erkekler göre daha fazla siber zorbalığa veya siber tacize maruz kalabilmektedir (Doğan vd., 2018). Bu durum kadın öğrencilerin bu ortamlarda daha bilinçli hareket etmesini ve siber güvenliğe yönelik farkındalıklarının yüksek olmasını sağlayabilir. Farklı olarak, Özbek (2019) erkek öğretmen adayların siber güvenlik farkındalıklarının kadın adaylardan yüksek olduğunu ifade etmiştir. Bu çalışmada da erkek öğrencilerin siber güvenlik farkındalıkları az da olsa kadınlardan yüksektir ama bu fark anlamlı değildir.

Bölüm farklılıklarına göre öğrencilerin siber güvenlik farkındalıkları incelendiğinde; tüm bölümlerde öğrenim gören öğrencilerin siber güvenlik farkındalıkları yüksek düzeydedir. Bilgisayar, elektronik, inşaat, makine ve mekatronik

gibi sayısal bilimlere ait bölümlerde alana özgü bilgisayar destekli birçok çevrimiçi veya masaüstü uygulamalar kullanılmaktadır. İşletme, iktisat, muhasebe ve halkla ilişkiler gibi sosyal bilimlere ait bölümlerde kişisel ve finans bilgilerinin yönetildiği bilgisayar destekli uygulamalara yer verilebilmektedir. Dolayısıyla MYO öğrencilerinin bilgi araçlarını yoğun bir şekilde kullanmaları ve bu konularda dijital okuryazar olmaları siber güvenliğe yönelik farkındalıklarını da artırabileceği düşünülmektedir. Bilgisayar Teknolojileri bölümü öğrencilerinin siber güvenlik farkındalıkları genellikle birçok bölüme göre olumlu yönde farklılık oluşturmuştur. Öğrencilerin genellikle teknolojiye ve dijital dünyaya oldukça ilgi duyması, siber güvenlik gibi önemli bir konuya karşı da duyarlı olmalarını sağlayabilir (Karacı vd., 2017). Çünkü bilgisayar ağları, internet programcılığı, web tasarımı, test ve otomasyon, sunucular ve siber güvenlik konularına öğretim programlarında yer verilebilmektedir. Bu durum onları, yazılım geliştirme sürecinde yazılımda karşılaşılabilecek güvenlik açıklarını, zafiyetlerini ve tehditlerini fark etme konusunda daha dikkatli hale getirebilir. Kendi yazılımlarını geliştirirken güvenliği göz önünde bulundurmak, onlara siber güvenlik farkındalığı kazandırabilir.

Turizm bölümünde öğrenim gören öğrencilerin siber güvenlik farkındalıkları; bilgisayar teknolojileri, işletme yönetimi ve halk ve ilişkiler bölümlerine göre anlamlı bir şekilde daha düşük çıkmıştır. Öğrencilerin sorumlu olduğu bölüm müfredatlarında siber güvenlik ve dijital güvenlik ile ilgili konular ve kavramlar diğer bölümlere göre daha sınırlı düzeyde yer almaktadır. Bu durum öğrenim sürecinde öğrencilerin siber güvenlik teknolojileriyle etkileşim düzeylerini de etkileyebilir. Dijital okuryazarlığın siber güvenlik ile ilgili farkındalığın oluşmasında önemli bir etkisi vardır (Altun ve Yukselturk, 2024). Turizm bölümü öğrencileri müfredatlarında genellikle seyahat, konaklama, pazarlama ve müşteri hizmetleri gibi konulara yoğunlaştıkları için siber güvenliğe olan ilgileri ve yönelimleri daha düşük olabilir. Turizm sektörü, dijital teknolojilerden giderek daha fazla faydalansa da bazı öğrenciler teknolojiyi sadece bir araç olarak görebilir ve bu nedenle siber güvenlik riskleri ve korunma yöntemleri hakkında derinlemesine bir anlayışa sahip olamayabilir. Halkla İlişkiler bölümü öğrencileri, dijital platformlar ve sosyal medya araçları ile sürekli etkileşim halindedir (Yavuz, 2017). Bu platformlar, siber güvenlik riskleri ve tehditleri için önemli bir alan oluşturabilir. Öğrenciler, çevrimiçi itibar yönetimi, kriz iletişimi ve sosyal medya kampanyaları gibi konuları öğrenirken, dijital güvenlik konularına da aşina olabilirler. Ayrıca halkla ilişkiler, genellikle müşteri verilerini, medya listesini, marka bilgilerini ve diğer hassas bilgileri yönetmeyi de ele alır (Koçyiğit, 2017). Bu durum siber güvenliğin ve veri korumanın önemini öğrencilere benimsetebilir. İşletme yönetimi bölümü öğrencilerinin siber güvenlik farkındalıklarının anlamlı bir şekilde yüksek olmasının nedenleri arasında; şirketlerin verimliliği artırmak, maliyetleri düşürmek ve müşteri hizmetlerini iyileştirmek amacıyla dijital teknolojilere yönelimleri gösterilebilir. Bu durum işletme yönetimi öğrencilerinin dijital sistemler, yazılımlar ve bulut hizmetleri gibi araçlarla sık sık etkileşimde bulunmalarına neden olabilir (Çalışkan, 2025). Teknolojinin bu kadar iç içe olması, siber güvenlik farkındalığının önemini öğrencilere kazandırabilir.

MYO öğrencilerinin daha çok 3 ile 5 saat arasında internette vakit geçirdikleri görülürken, internet kullanan öğrencilerin kullanım sıklığına bağlı olmaksızın siber güvenlik farkındalıkları yüksektir. Özbek (2019), interneti daha sık kullanan üniversite öğrencilerinin farkındalıklarının daha yüksek olduğunu belirtmiştir. İnternet kullanım süresi arttıkça öğrencilerin maruz kalacakları tehditler ve riskler daha fazla olabilir (Denis vd., 2023). MYO öğrencilerin üçte biri, interneti oyun amaçlı olarak kullandıklarını ifade etmişlerdir. Çevrimiçi olarak oynanan oyunlarda öğrenciler; etkileşimde bulunabilir, kişisel bilgilerini, e-posta adreslerini, ip adreslerini ve ödeme bilgilerini bu ortamlarda paylaşabilirler. Özellikle güvenlik önlemleri zayıf olan oyun platformlarında paylaşılan bu bilgiler kötü niyetli olarak kullanılabilir. Oyun içerisinde kurulan etkileşimler siber zorbalık, taciz ve nefret söylemleri gibi sorunları da beraberinde getirebilir. Yani çok fazla oyun ile vakit geçiren öğrenciler bu tür olumsuz durumlara maruz kalabilirken, edinilen bilgi ve deneyimler öğrencilerin siber güvenlik farkındalıklarına da katkı sağlamış olabilir.

Sonuçlar ve Öneriler

Bu çalışmada, MYO öğrencilerinin siber güvenlik farkındalıkları; cinsiyet, bölüm ve internet kullanım sıklığı çerçevesinde incelenmiştir. Ayrıca öğrencilerin internet kullanım amaçları belirlenerek siber güvenlik farkındalığına etkisi tartışılmıştır. Teknik ve sosyal bilimler ile ilgili farklı bölümlerde öğrenim gören öğrencilerin siber güvenlik farkındalıkları yüksek düzeydedir. Bölümlerde bilgisayar destekli derslerin yer alması, dijital teknolojilerin alana entegrasyonu, çevrimiçi araçlar ile etkileşim yaşanması, bilgi edinme ve sosyal medya kullanımı amacıyla internet kullanımının yaygınlaşması öğrencilerin siber güvenliğe yönelik farkındalığını etkileyen unsurlar arasında sayılabilir. Özellikle bilgisayar teknolojileri, işletme yönetimi ve halkla ilişkiler bölümü öğrencilerinin farkındalıkları diğer bölümlerden pozitif olarak farklılaşmıştır. Turizm bölümü öğrencilerinin siber güvenlik farkındalık düzeyi yüksek olmakla birlikte diğerlerine oranla daha düşüktür. Cinsiyet ve internet kullanım faktörü öğrencilerin farkındalık düzeylerini etkilememiştir. Öğrenciler, internetteki vakitlerinin çoğunu bilgi edinme, sosyal medya, oyun ve eğlence amaçlı olarak geçirmektedir. Dolayısıyla MYO öğrencileri dahil bir çok üniversite öğrencisi siber tehditlere, zorbalıklara ve tacizlere maruz kalabilir. Benzer şekilde akıllı telefon ve tabletler sayesinde internet kullanımının çok küçük yaşlara kadar düştüğü günümüzde farklı kademelerde öğrenim gören öğrencilerin de siber güvenlik farkındalıkları ve uygulamaları belirlenebilir. Bu sayede politika yapıcılarının, yöneticilerin ve eğitimcilerin öğrencilerin siber güvenlik ihtiyaçlarını anlamalarına ve siber güvenliği teşvik etmek için stratejiler belirlemelerine yardımcı olunabilir. Farklı seviyelerde öğrenim gören öğrencilerin siber güvenlik ile ilgili algılarını geliştirmek ve farkındalıklarını artırmak için yüz yüze veya çevrimiçi teorik ve uygulamaya dayalı eğitimler düzenlenebilir. Birçok meslek grubunda süreçler dijital ortamlar

üzerinden yürütülürken, müşterilerin bilgileri bu ortamlarda tutulmaktadır. Dolayısıyla doğrudan meslek edindirmeye yönelik eğitim veren MYO'ların eğitim müfredatlarında siber güvenlik kavramlarına yer vermesi önemli görülmektedir.

Etik Kurul İzni

Bu araştırmanın, Ordu Üniversitesi Rektörlüğü Etik Komisyonu Kurulunun 25.10.2024 tarih ve 2024-149 sayılı kararı ile etik ilkelere uygun olduğu beyan edilmiştir.

Çıkar Çatışması

Çıkar çatışması yoktur.

Kaynaklar

- Aksoğan, M., Bayer, H., Gülada, M., & Çelik, E. (2018). İletişim fakültesi öğrencilerinin siber güvenlik farkındalığı: İnönü Üniversitesi örneği. *Kesit Akademi Dergisi*, 4(13), 271-288.
- Altun, O., & Yukselturk, E. (2024). Lise öğrencilerinin dijital okuryazarlık ve siber güvenlik farkındalıklarının incelenmesi. *Kırıkkale Üniversitesi Sosyal Bilimler Dergisi*, 14(2), 321-346.
- Arıca, O. T. (2011). Siber zorbalık: Gençlerimizi Bekleyen Yeni Tehlike. *Kariyer Penceresi*, 2(6), 10-12.
- Arıca, O. T., Tanrikulu, T., & Kınay, H. (2012). Siber mağduriyet ölçeği'nin ilk psikometrik bulguları. *Akdeniz Eğitim Araştırmaları Dergisi*, 11, 1-6. <https://doi.org/10.29329/MJER>.
- Arpaci, I., & Sevinc, K. (2022). Development of the cybersecurity scale (CS-S): Evidence of validity and reliability. *Information Development*, 38(2), 218-226. <https://doi.org/10.1177/0266666921997512>.
- Aslan, T. (2020). *Üniversite öğrencilerinin sosyal medya kaygılarının sosyal medya bağımlılıklarını yordayıcı rolünün incelenmesi* [Yayınlanmamış Yüksek Lisans Tezi]. Çag Üniversitesi.
- Bada, M., Sasse, A.M., Nurse, J.R. (2019). Cyber security awareness campaigns: why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*. <https://doi.org/10.48550/arXiv.1901.02672>
- Barlett, C. P., & Chamberlin, K. (2017). Examining cyberbullying across the lifespan. *Computers in Human Behavior*, 71, 444-449. <https://doi.org/10.1016/j.chb.2017.02.009>
- Barrett, M. P. (2018). Framework for improving critical infrastructure cybersecurity, version 1.1. *National Institute of Standards and Technology (2018)*. <https://doi.org/10.6028/nist.cswp.04162018>.
- Bhatnagar, N., & Pry, M. (2020). Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. *Information Systems Education Journal*, 18(1), 48-58.
- Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, 70, 291-302. <https://doi.org/10.1016/j.chb.2017.01.003>
- Çalışkan, T. (2025). *Dijital dönüşüm sürecinde siber güvenlik farkındalığı: Konya'da bilişim sektöründe faaliyet gösteren kobiler üzerine bir araştırma* [Yayınlanmamış Yüksek Lisans Tezi]. Necmettin Erbakan Üniversitesi.
- Denis, N., Laurent, M., & Chabridon, S. (2023). Integrating usage control into distributed ledger technology for internet of things privacy. *IEEE Internet of Things Journal*, 10(22), 20120-20133. <https://doi.org/10.1109/jiot.2023.3283300>
- Doğan, B. Ö., Ertürk, Y. D., & Aslan, P. (2018). Facebook kullanıcısı kız çocuklarına yönelik zorbalık odaklı siber tacizin cinsel tacize dönüşümü: Gazete haberleri üzerinden betimsel bir değerlendirme. *Etkileşim*, (2), 36-55. <https://doi.org/10.32739/etkilesim.2018.2.27>
- Eroğlu, Y. (2014). *Ergenlerde Siber Zorbalık ve Mağduriyeti Yordayan Risk Etmenlerini Belirlemeye Yönelik Bütüncül Bir Model Önerisi* [Yayınlanmamış Yüksek Lisans Tezi]. Uludağ Üniversitesi.
- Fraenkel, J. R. & Wallen, N. E. (2006). *How to design and evaluate research in education*. (6th edition). MrGraw-Hill International Edition.
- Hatipoğlu, C., & Tunacan, T. (2021). Türkiye'de siber saldırı ve tespit yöntemleri: Bir literatür taraması. *Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi*, 8(1), 430-445. <https://doi.org/10.35193/bseufbd.838732>
- International Telecommunication Union (2008). International Telecommunication Union, ITU-TX.1205: Series X:Data networks, open system communications and security: Telecommunication security: Overview of cybersecurity. <https://www.itu.int/rec/T-REC-X.1205-200804-I>
- Kalaycı, Ş. (2016). *SPSS uygulamalı çok değişkenli istatistik teknikleri* (7th ed.). Ankara: Asil Yayın Dağıtım.
- Karacı, A., Akyüz, H. İ., & Bilgici, G. (2017). Üniversite Öğrencilerinin Siber Güvenlik Davranışlarının İncelenmesi. *Kastamonu Eğitim Dergisi*, 25(6), 2079-2094. <https://doi.org/10.24106/kefdergi.351517>
- Koçyiğit, M. (2017). Halkla ilişkiler algısının marka imajı ve marka bağlılığı üzerindeki etkisi. *Selçuk İletişim*, 10(1), 85-97. <https://doi.org/10.18094/josc.330935>
- Korkmaz, A. (2016). Siber zorbalık davranışları sergileme ve siber zorbalığa maruz kalma durumlarının karşılaştırılması. *TRT akademi*, 1(2), 620-639.
- Kovačević, A., Putnik, N., & Tošković, O. (2020). Factors related to cyber security behavior. *IEEE Access*, 8(1), 125140-125148. <https://doi.org/10.1109/ACCESS.2020.3007867>
- Moallem, A. (2019). Cyber security awareness among college students. In *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, July 21-25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA 9* (pp. 79-87). Springer International Publishing.
- Özbek, Y. (2019). *Öğretmen adaylarının siber güvenlik farkındalıklarının incelenmesi* [Yayınlanmamış Yüksek Lisans Tezi]. Necmettin Erbakan Üniversitesi.
- Özer Öksüzöğlu, T. Ö. (2021). Kadınlara yönelik siber zorbalık durumları ve önlem çalışmaları. *European Journal of Educational and Social Sciences*, 6(1), 67-75.
- Salem, Y., Moreb, M., & Rabayah, K. S. (2021). Evaluation of information security awareness among palestinian learners. In *2021 International Conference on Information Technology (ICIT)* (pp. 21-26). Amman, Jordan, IEEE.
- Süslü, D. P. (2016). *Lise Öğrencilerinde Siber Zorbalık ve Siber Mağduriyetin Benlik Saygısı Anne, Baba ve Akran İlişkileri Açısından İncelenmesi* [Yayınlanmamış Doktora Tezi]. Maltepe Üniversitesi.

- Şener, H., Arıkan, İ., & Gülekçi, Y. (2022). Covid-19 pandemisinde üniversite öğrencilerinin siber güvenlik farkındalıkları ile siber zorbalık ve siber mağduriyet düzeylerinin değerlendirilmesi. *Bull Leg Med*, 27(2), 142-149. <https://doi.org/10.17986/blm.1577>
- Şimşek, T. (2024). Planlı davranış teorisi kapsamında a/b kişilik tipine göre siber güvenlik farkındalığı: Üniversite öğrencileri üzerine araştırma. *MANAS Sosyal Araştırmalar Dergisi*, 13(3), 1066-1074. <https://doi.org/10.33206/mjss.1300491>
- Teddlie, C., & Yu, F. (2007). Mixed methods sampling: A typology with examples. *Journal of Mixed Methods Research*, 1(1), 77-100. <https://doi.org/10.1177/2345678906292430>
- Türk, B., & Şenyuva, G. (2021). Şiddet sarmalı içinden siber zorbalık: Bir gözden geçirme. *IBAD Sosyal Bilimler Dergisi*, (10), 462-479. <https://doi.org/10.21733/ibad.901032>
- Yaman, E., & Sönmez, Z. (2015). Ergenlerin siber zorbalık eğilimleri. *Online Journal of Technology Addiction and Cyberbullying*, 2(1), 18-31.
- Yavuz, C. (2017). Meslek yüksekokulları halkla ilişkiler programı öğrencilerinin sosyal medya kullanımı alışkanlığı: Ordu Üniversitesi örneği. *MANAS Sosyal Araştırmalar Dergisi*, 6(2), 169-181.
- Yiğit, M. F., & Seferoğlu, S. S. (2019). Öğrencilerin siber güvenlik davranışlarının beş faktör kişilik özellikleri ve çeşitli diğer değişkenlere göre incelenmesi. *Mersin Üniversitesi Eğitim Fakültesi Dergisi*, 15(1), 186-215. <https://doi.org/10.17860/mersinefd.437610>

Extended Abstract

Purpose

This study aims to determine the awareness levels of vocational school students regarding cybersecurity. In this context, the following research questions were sought:

How do the cybersecurity awareness levels of vocational school students change depending on gender?

1. How do the cybersecurity awareness levels of vocational school students change depending on their departments?
2. How do the cybersecurity awareness levels of vocational school students change depending on their internet usage frequency?
3. How do the purposes of vocational school students use the internet vary?

Method

The research was conducted using the scanning method, which is among the quantitative studies. The sample of the research consisted of vocational school students studying in the technical and social sciences departments of the university in the city center and districts of Ordu. Students were categorized according to gender, department and Internet usage frequency. The Cyber Security Scale developed by Arpacı and Sevinc (2022) was used as the data collection tool. The Cronbach's alpha internal consistency coefficient of the scale was 0.88. While collecting the scale data, demographic information was also collected in order to reveal the purpose of students' Internet usage. The options included education and research, social media, entertainment and other. The other option was open-ended.

Results

The results of this study revealed the following.

Depending on gender, department and Internet usage frequency, vocational school students had high cyber security awareness levels (high level score range: 86-105).

According to the Mann-Whitney U test results, male students' test scores (Avg.=98.5) were higher than female students' test scores (Avg.=97), but the results did not reveal a significant difference ($U=18081.5$, $p>0.05$).

According to the Kruskal-Wallis test results, students' Internet usage frequency was one to three hours (Avg.=99), more than five hours (Avg.=98) and three to five hours (Avg.=97). Despite these differences between the scores, these results did not reveal a significant difference ($H(2)=4.455$, $p>0.05$).

According to the Kruskal-Wallis test results, there was a significant difference between students' cybersecurity awareness depending on the departments ($H(8)= 26.921$, $p<0.05$). When the significant differences between the departments were examined, the cybersecurity awareness of the computer department students was generally higher than that of the other departments. The cybersecurity awareness of the tourism department students was generally lower.

403 students were asked to mark their Internet usage purposes during the scale filling process. Approximately 10 percent of the students ($N=35$) did not spend time on the Internet for any purpose. 38 percent of the students ($N=152$) obtained information from the Internet. Almost half of the students used social media ($N=196$, 48%). Around 30% of students used the Internet for gaming and entertainment purposes ($N=126$, 31%).

Discussion, Conclusion, and Suggestions

38 percent of students use the internet for information purposes. Although there are many reliable sites that provide information, many websites also provide malicious information. During this process, most students may have positive or negative experiences. Experiences can be effective in increasing students' cybersecurity awareness and awareness levels. The literature states that university students are aware of threats to privacy and security that may arise from social media (Bhatnagar & Pry, 2020).

It has been observed that there is no difference between the cybersecurity awareness of vocational school students depending on gender, but both have high awareness levels. While some studies state that gender is not effective (Karacı et al., 2017; Korkmaz, 2016), others emphasize that gender is effective (Özbek, 2019). In a different way, Özbek (2019) stated that male teacher candidates have higher cybersecurity awareness than female candidates. In this study, male students' cybersecurity awareness is slightly higher than that of female students, but this difference is not significant.

When the cyber security awareness of students was examined according to department differences, the cybersecurity awareness of students studying in all departments was high. Many computer-supported online or desktop applications specific to the field are used in departments of numerical sciences such as computer, electronics, construction, machinery and mechatronics. The fact that students are generally very interested in technology and the digital world may also make them sensitive to an important issue such as cyber security (Karacı et al., 2017). The cybersecurity awareness of students studying in the tourism department was found to be significantly lower than those studying in the computer technologies, business administration and public relations departments. Since tourism department students generally focus

on issues such as travel, accommodation, marketing and customer service, their interest in and orientation towards cybersecurity may be lower. Public Relations department students may be in constant interaction with digital platforms and social media tools (Yavuz, 2017). These platforms may constitute an important area for cybersecurity risks and threats.

While vocational school students spend more time on the Internet between three and five hours, students who use the Internet have high cybersecurity awareness regardless of the frequency of use. Özbek (2019) stated that university students who use the Internet more frequently have higher awareness. As the duration of Internet use increases, the threats and risks that students are exposed to may increase (Denis et al., 2023). While students who spend too much time playing games may be exposed to negative situations, the knowledge and experiences gained may also contribute to students' cybersecurity awareness.

In today's World, where Internet use has decreased to very young ages thanks to interactive phones and tablets, cybersecurity awareness and practices of students studying at different levels can be determined. In this way, it can help policymakers, administrators and educators understand the cybersecurity needs of students and determine strategies to promote cybersecurity.